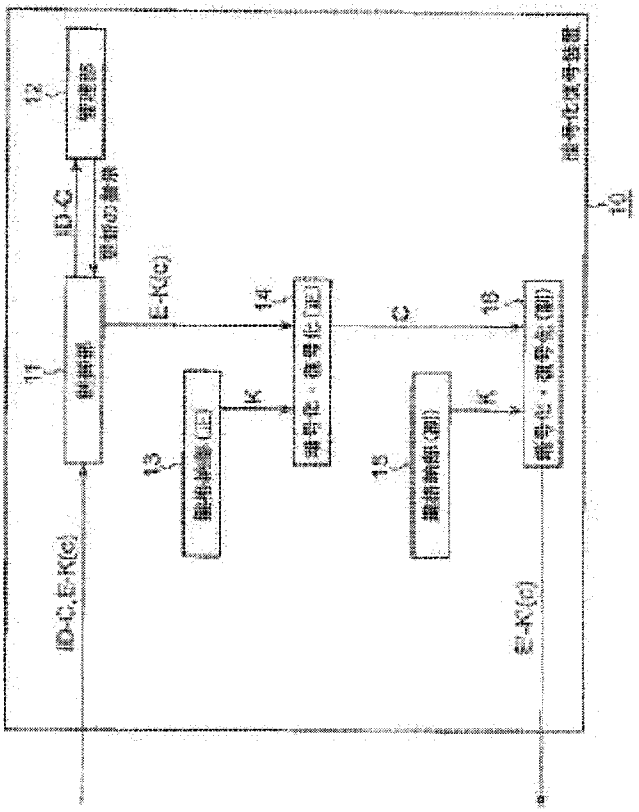
ENCIPHERING/DECIPHERING DEVICE AND CIPHER SYSTEM CHANGING METHOD

Publication number: JP2002281016 (A)
Publication date: 2002-09-27
Inventor(s): TOCHIKUBO TAKAYA; OKADA KOJI; ENDO NAOKI
Applicant(s): TOKYO SHIBAURA ELECTRIC CO
Classification:
- international: ***H04L9/10; H04L9/14;*** **H04L9/10; H04L9/14;** (IPC1-7): H04L9/10; H04L9/14
- European:
Application number: JP20010078283 20010319
Priority number(s): JP20010078283 20010319

Abstract of **JP 2002281016 (A)**

PROBLEM TO BE SOLVED: To safety and efficiently change the cipher system of data. SOLUTION: The enciphering/deciphering device is provided with a management part 12 capable of managing the identification information of enciphered data and the information of the cipher system and a key, and deciding the necessity of the rewriting of the cipher system for each enciphered data, a key storing means (main) 13 for storing a key for decoding, an enciphering/ deciphering means (main) 14 for deciphering the enciphered data by the present cipher system by using the key in the key storing means (main), a key storing means (sub) 15 for storing a key for re-encipherment of the data deciphered by the ciphering/deciphering means (main), a key storing means (sub) 16 for re-ciphering the data by a new cipher system by using the key in the key storing means (sub),; and a control part 11 for transmitting the inputted enciphered data to the enciphering/deciphering means (main), and for controlling the enciphering/deciphering means (main) based on the decided contents of a managing means to output the deciphered data, or to transmit the data to the enciphering/deciphering means (sub).



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－281016
（P2002－281016A）
(43)公開日　平成14年９月27日(2002.9.27)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ａ	５Ｊ１０４
9/14			６４１	

審査請求　未請求　請求項の数６　ＯＬ　（全　６　頁）

(21)出願番号　特願2001－78283(P2001－78283)

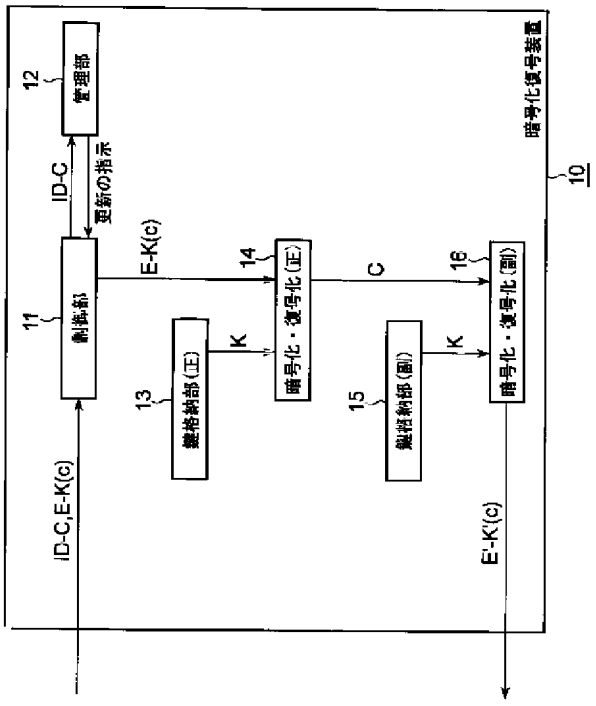
(22)出願日　平成13年３月19日(2001.3.19)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　栃窪　孝也
東京都府中市東芝町１番地　株式会社東芝府中事業所内
(72)発明者　岡田　光司
東京都府中市東芝町１番地　株式会社東芝府中事業所内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　暗号化復号装置及び暗号方式変更方法

(57)【要約】
【課題】　データの暗号方式を安全且つ効率良く変更する。
【解決手段】　暗号化データの識別情報、暗号方式及び鍵の情報を管理し、暗号化データ毎に暗号方式の書換の必要性を判定可能な管理部１２と、復号用の鍵が格納された鍵格納手段（正）１３と、鍵格納手段（正）内の鍵を用いて、現行の暗号方式により、暗号化データを復号する暗号化・復号手段（正）１４と、暗号化・復号手段（正）により復号されたデータの再暗号化用の鍵が格納された鍵格納手段（副）１５と、鍵格納手段（副）内の鍵を用いて、新規の暗号方式により、データを再暗号化する暗号化・復号手段（副）１６と、入力された暗号化データを暗号化・復号手段（正）に送出すると共に、この暗号化・復号手段（正）を管理手段の判定内容に基づいて制御し、復号により得られたデータを出力させるか又は暗号化・復号手段（副）に送出させる制御部１１を備えている。



【特許請求の範囲】
【請求項１】　暗号化データを復号し、得られたデータを出力又は再暗号化する暗号化復号装置であって、
暗号化データの識別情報、暗号方式及び鍵の情報を管理し、暗号化データ毎に、暗号方式の書換の必要性を判定可能な管理手段と、
暗号化データの復号に用いる鍵が格納された鍵格納手段（正）と、
前記鍵格納手段（正）内の鍵を用いて、現行の暗号方式により、前記暗号化データを復号する暗号化・復号手段（正）と、
前記暗号化・復号手段（正）により復号されたデータの再暗号化に用いる鍵が格納された鍵格納手段（副）と、
鍵格納手段（副）内の鍵を用いて、新規の暗号方式により、前記データを再暗号化する暗号化・復号手段（副）と、
暗号化データが入力されたとき、この暗号化データを前記暗号化・復号手段（正）に送出すると共に、この暗号化・復号手段（正）を前記管理手段の判定内容に基づいて制御し、復号により得られたデータを出力させるか又は暗号化・復号手段（副）に送出させる制御手段と、
を備えたことを特徴とする暗号化復号装置。
【請求項２】　請求項１に記載の暗号化復号装置を用いた暗号方式変更方法において、
前記暗号化データの暗号方式を変更する際に、前記暗号化データ及び前記識別情報が入力されるステップと、
前記識別情報に関連する管理内容に基づいて、当該暗号化データの暗号方式の書換の必要性を判定するステップと、
前記判定結果に基づいて、当該暗号化データを復号して得たデータを再暗号化するステップと、
を含んでいることを特徴とする暗号方式変更方法。
【請求項３】　請求項２に記載の暗号方式変更方法において、
前記暗号化データの暗号方式を変更する際に、
前記鍵格納手段（副）には、予め再暗号化に用いる鍵が格納されていることを特徴とする暗号方式変更方法。
【請求項４】　請求項２に記載の暗号方式変更方法において、
前記暗号化データの暗号方式を変更する際に、
前記暗号化・復号手段（副）には、予め新規の暗号方式が格納されていることを特徴とする暗号方式変更方法。
【請求項５】　請求項２に記載の暗号方式変更方法において、
前記管理されている全ての暗号化データの暗号方式が変更されたとき、前記暗号化・復号手段（正）を前記暗号化・復号手段（副）に、暗号化・復号手段（副）を暗号化・復号手段（正）に入れ替えるステップと、
前記入れ替えの完了後、暗号化・復号手段（副）の内容を消去するステップと、
を含んでいることを特徴とする暗号方式変更方法。
【請求項６】　請求項２に記載の暗号方式変更方法において、
前記管理されている全ての暗号化データの暗号方式が変更されたとき、前記鍵格納手段（正）を前記鍵格納手段（副）に、前記鍵格納手段（副）を前記鍵格納手段（正）に入れ替えるステップと、
前記入れ替えの完了後、鍵格納手段（副）の内容を消去するステップと、
を含んでいることを特徴とする暗号方式変更方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データの暗号化・復号を行なう暗号化復号装置及び暗号方式変更方法に係り、特に、データの暗号化方式を安全且つ効率良く変更し得る暗号化復号装置及び暗号方式変更方法に関する。
【０００２】
【従来の技術】近年、例えばコンテンツ配信事業や電子商取引といった一種の暗号システムでは、音楽・映像のコンテンツデータや電子マネー、電子バリューといったデータが暗号化されてハードディスクやＩＣカード等の記録装置に記録される。
【０００３】この種の暗号システムでは、利用者側でデータを復号して利用したり、再度、暗号化して記録装置へ書込む際には、所定の暗号方式により、データを暗号化・復号可能な利用者端末として暗号化復号装置が用いられている。
【０００４】このような暗号化復号装置は、多くの場合、所定の暗号方式が固定されている。しかしながら、安全な暗号通信のため、暗号方式は変更可能なことが望ましい。また、暗号方式を変更可能な暗号化復号装置でも暗号方式を安全かつ効率よく切り替えられないという問題がある。
【０００５】
【発明が解決しようとする課題】以上説明したように従来の暗号化復号装置では、多くの場合、所定の暗号方式が固定されており、また、暗号方式を変更可能な暗号化復号装置でも暗号方式を安全かつ効率よく切り替えられないという問題がある。
【０００６】本発明は上記実情を考慮してなされたもので、データの暗号方式を安全且つ効率良く変更し得る暗号化復号装置及び暗号方式変更方法を提供することを目的とする。
【０００７】
【課題を解決するための手段】第１の発明は、暗号化データを復号し、得られたデータを出力又は再暗号化する暗号化復号装置であって、暗号化データの識別情報、暗号方式及び鍵の情報を管理し、暗号化データ毎に、暗号方式の書換の必要性を判定可能な管理手段と、暗号化データの復号に用いる鍵が格納された鍵格納手段（正）

と、前記鍵格納手段（正）内の鍵を用いて、現行の暗号方式により、前記暗号化データを復号する暗号化・復号手段（正）と、前記暗号化・復号手段（正）により復号されたデータの再暗号化に用いる鍵が格納された鍵格納手段（副）と、鍵格納手段（副）内の鍵を用いて、新規の暗号方式により、前記データを再暗号化する暗号化・復号手段（副）と、暗号化データが入力されたとき、この暗号化データを前記暗号化・復号手段（正）に送出すると共に、この暗号化・復号手段（正）を前記管理手段の判定内容に基づいて制御し、復号により得られたデータを出力させるか又は暗号化・復号手段（副）に送出させる制御手段と、を備えた暗号化復号装置である。

【０００８】第２の発明は、第１の発明の暗号化復号装置を用いた暗号方式変更方法において、前記暗号化データの暗号方式を変更する際に、前記暗号化データ及び前記識別情報が入力されるステップと、前記識別情報に関連する管理内容に基づいて、当該暗号化データの暗号方式の書換の必要性を判定するステップと、前記判定結果に基づいて、当該暗号化データを復号して得たデータを再暗号化するステップと、を含んでいる暗号方式変更方法である。

【０００９】従って、データの暗号方式を変更する際には、２つの暗号化・復号手段（正）（副）を用い、各暗号化データを復号した後に他の暗号方式により再暗号化するので、データの暗号方式を安全且つ効率良く変更することができる。

【００１０】なお、前記暗号化データの暗号方式を変更する際に、前記鍵格納手段（副）には、予め再暗号化に用いる鍵が格納されていてもよく、また、前記暗号化・復号手段（副）には、予め新規の暗号方式が格納されていてもよい。

【００１１】また、前記管理されている全ての暗号化データの暗号方式が変更されたとき、前記暗号化・復号手段（正）を前記暗号化・復号手段（副）に、暗号化・復号手段（副）を暗号化・復号手段（正）に入れ替えるステップと、前記入れ替えの完了後、暗号化・復号手段（副）の内容を消去するステップと、を含んでいてもよい。

【００１２】同様に、前記管理されている全ての暗号化データの暗号方式が変更されたとき、前記鍵格納手段（正）を前記鍵格納手段（副）に、前記鍵格納手段（副）を前記鍵格納手段（正）に入れ替えるステップと、前記入れ替えの完了後、鍵格納手段（副）の内容を消去するステップと、を含んでいてもよい。

【００１３】

【発明の実施の形態】以下、本発明の一実施形態について図面を用いて説明する。なお、本実施形態においては、暗号化されたデータをＥ-ｘ（ｙ）で表す。ここで、ｘは暗号化に用いる鍵ｘを表し、ｙは暗号化対象のデータｙを表す。

【００１４】図１は本発明の一実施形態に係る暗号化復号装置の構成を示すブロック図である。この暗号化復号装置１０は、制御部１１、管理部１２、鍵格納部（正）１３、暗号化・復号部（正）１４、鍵格納部（副）１５、暗号化・復号部（副）１６を備えている。

【００１５】ここで、制御部１１は、入力された暗号化データＥ-Ｋ（Ｃ）及びその識別情報ＩＤ-Ｃのうち、データの識別情報ＩＤ-Ｃを管理部１２に出力し、暗号化データＥ-Ｋ（Ｃ）を暗号化・復号部（正）１４に出力する機能と、管理部１２から更新の指示に基づき、暗号化・復号部（正）（副）１４，１６を制御して暗号化データを新規の暗号方式に書換える機能とをもっている。

【００１６】識別情報ＩＤ-Ｃは、例えばシリアル番号、暗号方式及び鍵情報を含むデータであり、暗号化データＥ-Ｋ（Ｃ）がコンテンツデータの場合、コンテンツのヘッダに配置されることが処理の容易性の観点から好ましい。

【００１７】管理部１２は、各暗号化データ毎にシリアル番号、暗号方式及び鍵情報を管理する機能と、各部１３～１６の暗号方式を管理する機能と、制御部１１から受けた識別情報ＩＤ-Ｃに基づいて、データの暗号化に使用される暗号方式の情報、鍵の情報を確認し、暗号方式の変更が必要なとき、制御部１１に更新の指示を出す機能と、全ての暗号化データの暗号方式が変更された後、暗号化・復号部（正）（副）１４，１６及び鍵格納部（正）（副）１３，１５を入れ替えて現行の暗号方式を消去する機能とを持っている。なお、暗号方式の変更が必要な時は、例えば管理される全ての暗号化データの中に、現行の暗号方式と、新規の暗号方式とが混在しているときである。

【００１８】鍵格納部（正）１３は、予め現行の暗号方式の鍵が格納されるメモリであり、暗号化・復号部（正）１４により読出可能となっている。

【００１９】暗号化・復号部（正）１４は、鍵格納部（正）１３内の鍵Ｋに基づいて、制御部１１から受けた暗号化データＥ-Ｋ（Ｃ）を復号し、得られた元データＣを暗号化・復号部（副）１６に出力する機能をもっている。

【００２０】鍵格納部（副）１５は、予め新規の暗号方式の鍵が格納されるメモリであり、暗号化・復号部（副）１６により読出可能となっている。

【００２１】暗号化・復号部（副）１６は、鍵格納部（副）１５内の新規の暗号方式の鍵Ｋ’により元データＣを暗号化し、新規の暗号方式による暗号化データＥ’-Ｋ’（Ｃ）を出力する機能とをもっている。

【００２２】なお、鍵格納部（副）１５及び暗号化・復号部（副）１６は、ハードウェアで作成される場合、チップの交換により設けてもよい。

【００２３】次に、以上のように構成された暗号化復号装置の動作を説明する。

【００２４】(復号手順) 制御部１１は、図２に必要な部分を示すように、例えば図示しない記録装置から読み出した暗号化データＥ-Ｋ（Ｃ）を暗号化・復号部（正）１４に出力する。暗号化・復号部（正）１４は、鍵格納部（正）１３から読み出した鍵ＫによりＥ-Ｋ（Ｃ）を復号し、元データＣを出力する。

【００２５】(暗号化変更手順) 制御部１１は、図１に示すように、図示しない記録装置から暗号化データＥ-Ｋ（Ｃ）及びその識別情報ＩＤ-Ｃを読み出す。また、制御部１１は、これら暗号化データＥ-Ｋ（Ｃ）及びその識別情報ＩＤ-Ｃのうち、データの識別情報ＩＤ-Ｃを管理部１２に出力し、暗号化データＥ-Ｋ（Ｃ）を暗号化・復号部（正）１４に出力する。

【００２６】管理部１２は、この暗号化データの識別情報ＩＤ-Ｃに基づいて、データの暗号化に使用される暗号方式の情報、鍵の情報を確認して暗号方式の変更の必要性を判定し、暗号方式の変更が必要なとき、制御部１１に更新の指示を出し、変更の必要がない場合は、処理を終了する。

【００２７】制御部１１は、更新の指示を受けると、以下のように、暗号化・復号部（正）（副）１４，１６を制御し、その後、暗号化・復号部（正）（副）１４，１６及び鍵格納部（正）（副）１３，１５を入れ替えてから現行の暗号方式を消去する。

【００２８】すなわち、暗号化・復号部（正）１４は、鍵格納部（正）１３内の鍵Ｋに基づいて、制御部１１から受けた暗号化データＥ-Ｋ（Ｃ）を復号し、元データＣを暗号化・復号部（副）１６に出力する。

【００２９】暗号化・復号部（副）１６は、鍵格納部（副）１５内の新規の暗号方式の鍵Ｋ’により元データＣを暗号化し、新規の暗号方式による暗号化データＥ’-Ｋ’（Ｃ）を記録装置に上書きする。

【００３０】以下、制御部１１は、順次、記録装置内の暗号化データＥ-Ｋ（Ｃｉ）を読み出して、新規の暗号方式による暗号化データＥ’-Ｋ’（Ｃｉ）に変更し、この暗号化データＥ’-Ｋ’（Ｃ）を記録装置に上書きする。

【００３１】また、管理部１２は、登録している全てのデータの暗号方式が新規の暗号方式に変更された時点で、現行の暗号化・復号部（副）１６を新規の暗号化・復号部（正）に、現行の暗号化・復号部（正）１４を新規の暗号化・復号部（副）に入れ替え、この新規の暗号化・復号部（副）の内容を消去する。

【００３２】また同様に、管理部１２は、現行の鍵格納部（副）１６を新規の鍵格納部（正）に、現行の鍵格納部（正）１３を新規の鍵格納部（副）に入れ替え、新規の鍵格納部（副）の内容を消去する。

【００３３】上述したように本実施形態によれば、データの暗号方式を変更する際には、２つの暗号化・復号部（正）（副）!4，１６を用い、各暗号化データを復号した後に新規の暗号方式により再暗号化するので、データの暗号方式を安全且つ効率良く変更することができる。

【００３４】また、管理部１２が各暗号化データの暗号方式を管理し、現行の暗号方式と、新規の暗号方式とが混在した場合には、全て新規の暗号方式に書換える必要性が有ることを判定するので、常に新規の暗号方式を使用でき、安全性を向上させることができる。

【００３５】なお、上記各実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、光磁気ディスク（ＭＯ）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

【００３６】また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【００３７】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【００３８】さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【００３９】また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【００４０】尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【００４１】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【００４２】なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。また、各実施形態は可能な限り適宜組み合わせて実施してもよく、その場合、組み合わされた効果が得られる。さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成用件における適宜な組み合わせにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発

明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【００４３】その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【００４４】

【発明の効果】以上説明したように本発明によれば、データの暗号方式を安全且つ効率良く変更できる。

【図面の簡単な説明】

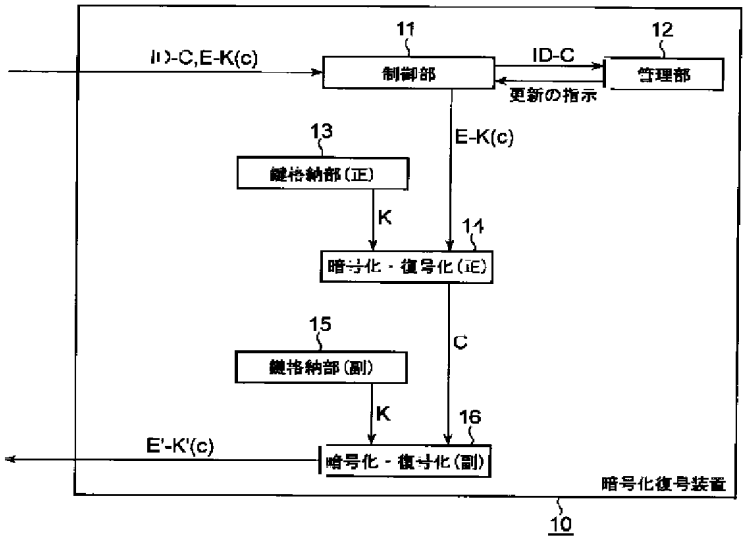
【図１】本発明の一実施形態に係る暗号化復号装置の構成を示すブロック図

【図２】同実施形態における動作を説明するための模式図

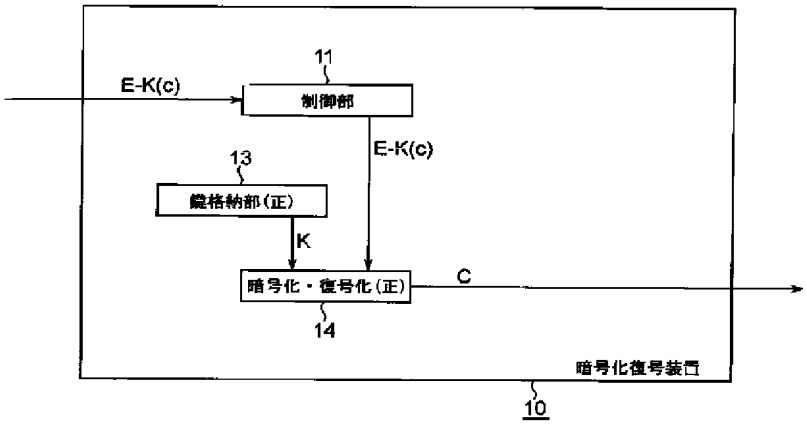
【符号の説明】

１０…暗号化復号装置
１１…制御部
１２…管理部
１３…鍵格納部（正）
１４…暗号化・復号部（正）
１５…鍵格納部（副）
１６…暗号化・復号部（副）

【図１】



【図２】



フロントページの続き

(72)発明者　遠藤　直樹
東京都府中市東芝町１番地　株式会社東芝
府中事業所内

Ｆターム(参考)　5J104 AA01 AA16 AA34 DA04 EA04
EA26 JA31 NA02 NA36 NA37